

42390P12196

PATENT

CLAIM AMENDMENTS:

1. (Currently amended) A method for on-connect security scan and delivery, comprising:
 - interfacing with a remote access infrastructure to detain a client in a virtual lobby when the client attempts to connect to a network;
 - scanning the client to determine if the client complies with security requirements;
 - and
 - permitting connection to the network only if the client complies with the security requirements;
 - performing a security risk assessment for the network; and
 - creating the security requirements to address risks identified in the security risk assessment.
2. (Original) The method as recited in claim 1, further comprising:
 - interfacing with at least one provider of at least one security mechanism to bring the client into compliance with the security requirements, if the client is not in compliance.
3. (Original) The method as recited in claim 1, further comprising:
 - retrieving client information from a repository.
4. (Canceled) Please cancel Claim 4 without prejudice.
5. (Currently amended) The method as recited in claim 1 4, further comprising:
 - storing the security requirements in a repository.
6. (Currently amended) The method as recited in claim 1 4, further comprising:
 - updating the security requirements with a new policy; and
 - interfacing with at least one provider to provide delivery of at least one security mechanism to at least partly implement the new policy.

42390P12196

PATENT

7. (Original) The method as recited in claim 6, further comprising:
certifying the at least one provider.
8. (Original) The method as recited in claim 6, further comprising:
storing the new policy in a repository.
9. (Original) The method as recited in claim 6, further comprising:
providing a custom configuration tool to at least partly implement the new policy.
10. (Canceled) Please cancel Claim 10 without prejudice.
11. (Canceled) Please cancel Claim 11 without prejudice.
12. (Canceled) Please cancel Claim 12 without prejudice.
13. (Canceled) Please cancel Claim 13 without prejudice.
14. (Currently amended) A method for on-connect security scan and delivery,
comprising:
controlling configuration of a plurality of security mechanisms for a client based
on security requirements for a network;
scanning the client for an indication of whether the client complies with the
security requirements;
providing a delivery assistant to the client to install and configure at least one of
the plurality of security mechanisms; and
permitting connection to the client, only if the client complies with the security
requirements; and
providing an optional delivery to the client.
15. (Original) The method as recited in claim 14, further comprising:

42390P12196

PATENT

certifying third-party security mechanisms that meet the security requirements;
and
distributing the certified third-party security mechanisms to the client through the
delivery assistant.

16. (Original) The method as recited in claim 14, further comprising:
storing client information, delivery information, and security requirements in a
repository.
17. (Canceled) Please cancel Claim 17 without prejudice.
18. (Currently amended) ~~The method as recited in claim 14, further comprising:~~ A
method for on-connect security scan and delivery, comprising:
controlling configuration of a plurality of security mechanisms for a client based
on security requirements for a network;
scanning the client for an indication of whether the client complies with the
security requirements;
providing a delivery assistant to the client to install and configure at least one of
the plurality of security mechanisms;
permitting connection to the client, only if the client complies with the security
requirements; and
presenting a security warning for the client.
19. (Original) The method as recited in claim 18, further comprising:
scheduling a future delivery for the client.
20. (Currently amended) A network security authority system, comprising:
a virtual lobby computing system in communication with two firewalls to protect
a network from insecure clients attempting to connect to the network;

42390P12196

PATENT

a scanning component operable on the computing system to determine if a client complies with security requirements and to determine if lacking security mechanisms are available for delivery; ~~and~~
a delivery component operable on the computing system to deliver available security mechanisms to the client; and
a repository component in communication with the computing system to store the security requirements, wherein the repository component is a database management system that operates to manage the security requirements and associated delivery instructions for available security mechanisms.

21. (Original) The network security authority system as recited in claim 20, further comprising:

a repository component in communication with the computing system to store the security requirements.

22. (Original) The network security authority system as recited in claim 21, wherein the repository component is a database management system.

23. (Canceled) Please cancel Claim 23 without prejudice.

24. (Original) The network security authority system as recited in claim 20, further comprising:

a certification system in communication with the computing system to certify third-party security mechanisms that meet the security requirements.

25. (Currently amended) An article of manufacture having instructions stored on it that cause a computing system to operate as a network security authority, the instructions comprising:

detaining a client that is attempting to connect to a network in a virtual lobby, the virtual lobby being between an outer firewall and an inner firewall, the inner firewall being between the virtual lobby and the network;

42390P12196

PATENT

providing resources for scanning the client to verify the client complies with security requirements;
providing implementation resources to help the client to comply with security requirements;~~and~~
denying permission for the client to connect to the network upon determining that the client does not comply with security requirements and that the implementation resources to bring the client into compliance are not available; and
scheduling later operations to bring the client into compliance for select security requirements.

26. (Original) The instructions as recited in claim 25, further comprising:
providing warnings for select security requirements and permitting the client to connect to the network; and
enforcing rules for overriding the select security requirements;
wherein the rules for overriding are adaptably defined under the circumstances.
27. (Canceled) Please cancel Claim 27 without prejudice.
28. (Original) The instructions as recited in claim 25, further comprising:
providing a presentation notifying the client of scanning.
29. (Original) The instructions as recited in claim 25, further comprising:
providing a presentation of implementation resources information to the client.
30. (Original) The instructions as recited in claim 25, further comprising:
providing a presentation of a compliance status to the client.
31. (Canceled) Please cancel Claim 31 without prejudice.
32. (Canceled) Please cancel Claim 32 without prejudice.

42390P12196

PATENT

33. (Canceled) Please cancel Claim 33 without prejudice.
34. (Canceled) Please cancel Claim 34 without prejudice.
35. (Canceled) Please cancel Claim 35 without prejudice.
36. (Canceled) Please cancel Claim 36 without prejudice.
37. (Canceled) Please cancel Claim 37 without prejudice.
38. (Canceled) Please cancel Claim 38 without prejudice.
39. (Canceled) Please cancel Claim 39 without prejudice.
40. (Canceled) Please cancel Claim 40 without prejudice.
41. (Canceled) Please cancel Claim 41 without prejudice.
42. (Canceled) Please cancel Claim 42 without prejudice.